# 基于遗传算法优化的 OCSVM 双轮廓模型异常检测算法 *

闫腾飞 [1, 2, 3]，尚文利 [2, 3, 4†]，赵剑明 [2, 3, 4]，乔　枫 [1]，曾　鹏 [2, 3, 4]

(1. 沈阳建筑大学 信息与控制工程学院, 沈阳 110168; 2. 中国科学院沈阳自动化研究所, 沈阳 110016; 3. 中科院网络化控制系统重点实验室, 沈阳 110016; 4. 中国科学院大学, 北京 100039)

**摘　要：**针对 Modbus 工业总线协议的特殊性及工控数据样本的不均衡性，利用单类支持向量机（OCSVM）分别构建正常 OCSVM 模型和异常 OCSVM 模型，即双轮廓模态，模拟系统通信的正常模式和异常模式，实现工控系统异常检测。同时将遗传算法优化自变量降维应用于工控网络入侵检测场景，实现对输入自变量的降维压缩处理，防止 OCSVM 模型出现过拟合现象及分类准确率低的问题，提高异常检测的精度，缩减建模时间，并通过仿真验证了提出算法对工控网络异常检测的有效性。

**关键词：**工业控制系统；异常检测；遗传算法；单类支持向量机；双轮廓模态

**中图分类号：**TP301.6　　doi: 10.3969/j.issn.1001-3695.2018.04.0313

## Anomaly detection algorithm based on OCSVM double contour model of genetic algorithm optimization for industrial control system

Yan Tengfei[1, 2, 3], Shang Wenli[2, 3, 4†], Zhao Jianming[2, 3, 4], Qiao Feng[1], Zeng Peng[2, 3, 4]

(1 *Faculty of Information & Control Engineering*, *Shenyang Jianzhu University*, *Shenyang* 110168, *China*; 2. *Shenyang Institute of Automation*, *Chinese Academy of Sciences*, *Shenyang* 110016, *China*; 3. *Key Laboratory of Networked Control Systems*, *Chinese Academy of Sciences*, *Shenyang* 110016, *China*; 3. *University of Chinese Academy of Sciences*, *Beijing* 100049, *China*)

**Abstract:** The Modbus industry bus protocol is special. And the network intrusion data sample of industrial control system is not balanced. So this paper used one-class support vector machine (OCSVM) to construct normal OCSVM model and abnormal OCSVM model to simulate the normal mode and abnormal mode of system communication. Then to realize the abnormal detection of industrial control system. In order to prevent the OCSVM model from overfitting and the low accuracy of classification, this paper used the genetic algorithm to the industrial control network by optimizing the dimensionality reduction of the independent variable. This method improves the accuracy of the anomaly detection and reduces the modeling time. Simulation results show that the proposed algorithm is effective for anomaly detection of industrial network.

**Key words:** industrial control system; anomaly detection; genetic algorithm; one-class support vector; double control model

## 0　引言

近年来，工业控制系统（industrial control system）与互联网的交互逐渐密切，工业控制进入智能时代。当前，除电力、石化、核设施等国家基础工业领域外，与民生密切相关的市政系统也分布了大量的工业控制系统。工业控制设备和工控通信协议从设计之初就对信息安全问题考虑不足，同时由于自身的脆弱性、各种漏洞和后门的存在，让工控系统信息安全隐患问题日益突出。

由于工控安全自身的特殊性，工业防火墙虽然实现了通信的访问控制和网络隔离[1]，但人工设置规则容易导致错误。同时网络安全中间件产品会影响系统的实时操作。现阶段，防火墙技术对网络的防护不足以应对大规模化的网络以及复杂化的入侵攻击 [2]。如何让工控安全从“被动防御”走向“主动防护”成为网络安全领域的首要问题。入侵检测技术作为一种主动防护技术，能够检测发现隐藏于流经网络边界正常信息流中的入侵行为[3]，分析潜在威胁并进行安全审计，所以可广泛应用于工控系统的网络安全中。

目前，异常入侵检测系统被广泛应用于工控安全主动防护中[4]。以往对异常检测的研究多采用机器学习的方法，其中支

**收稿日期：**2018-04-25；**修回日期：**2018-06-11　**基金项目：**国家自然科学基金面上项目（61773368）；预研基金资助项目（6140242010116Zk63001）

**作者简介：**闫腾飞（1990-），女，山东潍坊人，硕士研究生，主要研究方向为工业控制系统信息安全、入侵检测技术;：尚文利（1974-），男（通信作者），黑龙江北安人，研究员，博士，主要研究方向为工业控制系统信息安全、计算智能与机器学习（shangwl@sia.cn）；赵剑明（1987-），男，辽宁葫芦岛人，助理研究员，硕士，主要研究方向为网络安全；乔枫（1960-），男，辽宁沈阳人，教授，博士，主要研究方向为机电系统的系统建模与仿真、工业机器人运动控制、复杂动态系统控制；曾鹏（1976-），男，辽宁沈阳人，研究员，博士，主要研究方向为工业无线传感器、智能电网.

持向量机（support vector machine, SVM）在解决小样本、非线性及高维模式识别中具备特有的优势，因而广泛应用于工控异常检测中[5,6]。文献[4]利用 SVM 的分类方法建立工控通信协议数据检测模型，虽然能在一定程度上检测工业控制系统的异常通讯行为，但误报率仍然较高。由于单类支持向量机（OCSVM）仅需一类样本即可训练异常检测模型[3]，故可应用于工控网络异常检测系统。文献[7]提出了利用 OCSVM 检测入侵起源和时间节点，创建集群的入侵检测模型，提高了检测精度，但是实时性较差；文献[8]提出将 K-均值聚类方法与 OCSVM 相结合进行入侵检测，能够检测恶意网络流量，实现入侵检测，虽然在检测时间上有所提高，但是面对高维非线性的数据样本时，容易出现过拟合现象；文献[9]将 KICA 方法与 OCSVM 相结合，降低故障检测率，避免了初始值对分离矩阵的影响，从而缩短延迟时间。

为提高检测精度，需要对 OCSVM 参数 v 和核函数参数 g 进行寻优。常用的优化单类支持向量机参数方法主要有随机选取法、网格搜索法、粒子群算法、遗传算法等。传统的根据经验随机选取(v, g)的方法很难保证检测精度，具有较大的随机性，并且不能保证选择的参数是最优的。网格搜索法主要对 OCSVM 参数 v 和核函数参数 g 设置搜索范围和步长，确定二维网络，依据固定的步长进行寻优，在步长足够短且空间足够大时具有不错的寻优效果。但是网格搜索法寻优速度慢，而且容易获得局部最优解，严重影响 OCSVM 的检测效果和检测的实时性。粒子群算法对 OCSVM 参数寻优过程中，容易实现且需要调整的参数并不多，寻优速度快、检测时间短，但是容易陷入局部最优。遗传算法优化 OCSVM 参数虽然操作较复杂，需要进行选择、交叉、变异等操作，但是能够得到全局最优解，能够提高 OCSVM 模型的检测准确率。本文工作是在缩减检测时间的基础上提高检测精度，降低误报率和漏报率，因此选取遗传算法对 OCSVM 参数 v 和核函数参数 g 进行寻优。

对 Modbus 工业总线协议及工控数据样本的不均衡性，本文利用单类支持向量机（OCSVM）仅需一类样本即可训练异常检测模型的特点，分别构建正常 OCSVM 模型和异常 OCSVM 模型，即双轮廓模态，模拟系统通讯的正常模式和异常模式，实现工控系统异常检测。同时经过研究发现 OCSVM 模型由于输入自变量很多、输入自变量之间不相互独立，容易出现过拟合的现象，从而导致 OCSVM 模型检测精度低、建模时间长等问题。所以本文采用遗传算法对采集的工业数据进行特征约简去除冗余，选择最能反映输入与输出关系的自变量参与工控系统异常检测算法的建模，使得检测时间缩短，检测准确率得以提高。

## 1　Modbus TCP 通信协议分析及特征提取

工业控制系统是指面向于工业领域的控制系统，工控系统信息安全与传统 IT 网络信息安全之间具有较大差异性。其中，数据交换协议是较大的不同点。传统 IT 信息系统数据交换协议使用 TCP/IP 协议栈，而工控系统使用专用通信协议或规约，多采用 Modbus TCP 通信协议[10]。

Modbus 是一种工业现场总线协议标准，Modbus 协议是一项应用层报文传输协议，包括 ASCII、RTU、TCP 三种报文类型，协议本身没有定义物理层，只是定义了控制器能够认识和使用的消息结构[11]。Modbus 协议标准分为两类：串行链路上的 Modbus 和 TCP/IP 上的 Modbus。通过 Modbus TCP 报文传输协议，控制器相互之间通过网络（例如以太网）和其他设备之间通信[10]。Modbus TCP 报文传输服务结构如图 1 所示。

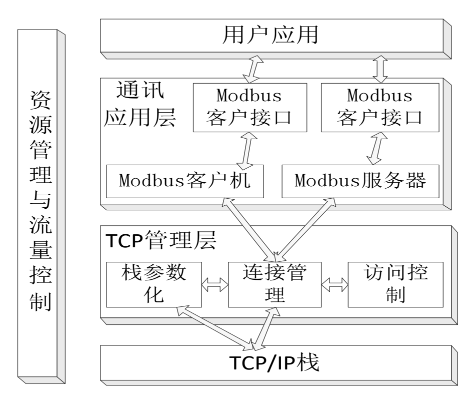



图 1　Modbus TCP 报文传输服务结构

实现完整的 Modbus TCP 通讯过程需要客户机建立一个连接，向服务器发送 Modbus 请求，客户机在收到应答之后正常地关闭连接。

Modbus TCP 协议定义了一个与基础通信层无关的简单协议数据单元（PDU），包括数据和功能码，特定总线或网线上的 Modbus 协议映射能够在应用数据单元（ADU）上引入一些附加码[12]。服务器对客户机响应时，使用功能码域来指示正常响应或异常响应[12]。提取入侵检测数据即对 Modbus TCP 数据帧进行处理。Modbus TCP 数据帧结构如下图 2。Modbus TCP 实现是在 TCP/IP 载荷内部包含了 Modbus 原有的校验数据。

| HDLC帧头 | 源/目的MAC | 源/目的IP | 载荷 |
| --- | --- | --- | --- |

| 起始 | 地址码 | 功能码 | 数据 | CRC | 结束 |
| --- | --- | --- | --- | --- | --- |
| 传输间隔 T1~T4 | 8位 | 8位 | N*8位 连续数据流 | 16位 | 传输间隔 T1~T4 |

图 2　Modbus TCP 帧结构

OCSVM 建立异常检测模型所需数据特征需要对 Modbus TCP 协议提取特征向量，包括从工控流量数据直接提取的地址码、长度、功能码、端口号、协议标识符、Modbus 长度等；以及根据异常行为模式结合实际工控流量进行构造的反映操作异常的检测特征，如单位时间内数据地址异常码数、连接设备标识数、读功能码数等。使用 Wireshark 软件截获数据报文，提取最能反映数据特征的属性构造特征向量，得到工控流量异常检测初始数据集。

## 2　单类支持向量机异常检测模型

工业异常检测数据样本正常数据多，异常数据少，样本呈

现不平衡性，如何在不平衡类别的异常数据上仍能取得较好的检测效果是关注的问题之一。One-Class 支持向量机解决一些只有一类的样本可用于训练分类器的情况。本文采用 OCSVM 分别建立正常模式和异常模式下的双轮廓模型，通过协同判别机制实时发现网络异常情况。

OCSVM 首先将输入空间通过核函数映射到高维空间，在高维空间将它们与原点尽可能分开。即寻求在特征空间构造一个最优超平面，假设坐标原点为异常样本，类别标签-1，正常样本类别标签+1，目标是确定正常样本的边界，即最优超平面，边界之外的数据被分为异常，实现正常工业数据与异常数据（坐标原点）的最大间隔。对于训练数据 $x$，$f(x)$表明它在高维空间位于超平面的正负方向，$f(x)$为正认为是正常类，反之则认为异常类。

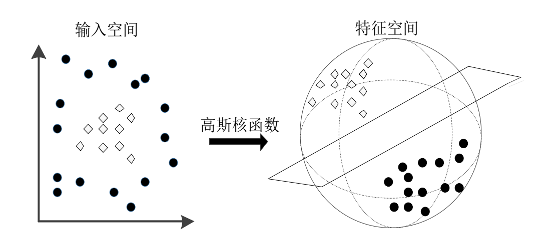



图 3　基于高斯核函数的 OCSVM 分类问题

当工控异常监测数据线性不可分时，引入核函数。本文使用高斯核函数，将数据从输入空间的非线性转变到特征空间转换成线性可分，这样就可以准确的对异常检测数据进行分类，如上图 3。若在二维空间，最优超平面即一条直线。

OCSVM 拟寻求最小化目标函数：

$$\min \frac{1}{2}\|\omega\|^2 + \frac{1}{vl}\sum_{i=1}^{l}\xi_i - \rho$$
$$s.t.\Phi(x_i)\omega \ge \rho - \xi_i, \xi_i \ge 0$$

其中：$x_i$ 为样本数据，$l$ 为训练集数量，$v$ 为权衡参数，$\Phi$ 为原始空间到特征空间映射，$\omega$ 和 $\rho$ 分别为特征空间中超平面的法向量和补偿。

引入拉格朗日函数：

$$L_p = \frac{1}{2}\|\omega\|^2 + \frac{1}{vl}\sum_{i=1}^{l}\xi_i - \rho - \sum_{i=1}^{l}\xi_i\beta_i - \sum_{i=1}^{l}(\Phi(x_i)\omega - \rho + \xi_i)\alpha_i$$

其中：$\alpha_i$、$\beta_i$ 为拉格朗日因子。引入高斯核函数将样本空间映射到特征空间得对偶问题：

$$K(x_i, x_j) = <\Phi(x_i), \Phi(x_j)> = \exp(-g\|x_i - x_j\|^2)$$

$$\min L = \frac{1}{2}\sum_{i=1}^{l}\sum_{j=1}^{l}a_i a_j K(x_i, x_j),\quad s.t. 0 \le a_i \le \frac{1}{vl}$$

由上式可求出 $\rho$：

$$\rho = \sum_{i=1}^{l}\alpha_i K(x_i, x_j)$$

求出决策函数即最优超平面，也就得到基于 OCSVM 的工业入侵检测模型：

$$f(x) = \mathrm{sgn}(\sum_{i=1}^{l}\alpha_i K(x_i, x_j) - \rho)$$

为得到较满意的异常检测模型，用 OCSVM 做分类测试需要调节响应参数（v, g）来得到理想的预测分类准确率，本文采用遗传算法进行参数寻优，取分类准确率作为适应度函数。

## 3　遗传算法优化自变量降维

本文遗传算法优化自变量降维建模选用工业入侵检测数据，包括异常检测标签（正常样本+1 和异常样本-1）、直接提取的特征（Modbus/TCP 长度、地址码、端口号等）和构造特征（单位时间内数据地址异常码数、连接设备标识数、数读功能码数等），共 21 个特征数据。显然，这 21 个输入自变量相互之间存在一定关系，并非相互独立。为缩短建模时间、提高建模精度，将除去检测标签后的 20 个输入自变量中起主要影响因素的自变量筛选出来参与最终建模[13]。

利用遗传算法进行优化计算，需要将解空间映射到编码空间，每个编码对应问题的一个解（即染色体或个体）。将编码长度设计为 20，染色体的每一位对应一个输入自变量。若染色体某一位为“1”，表示该位对应的输入自变量参与最终建模；反之，则表示“0”对应的输入自变量不作为最终自变量建模。本文对 Modbus/TCP 工业数据输入自变量降维选取测试集数据均方误差的倒数作为遗传算法的适应度函数，经过不断迭代筛选出最具有代表性的输入自变量参与 OCSVM 入侵检测模型的建模。遗传算法优化自变量降维流程图如图 4 所示。

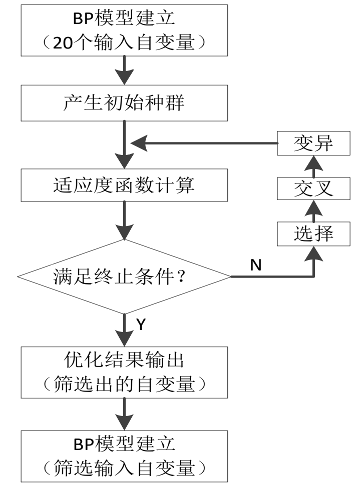



图 4 设计步骤

a)单 BP 模型构建。为了比较遗传算法优化前后预测的效果，先利用全部的 20 个输入自变量建立 BP 模型。

b)初始种群产生。产生随机的 $n$ 个初始数据，特点是具有串结构，每个具有串结构的数据作为一个个体，一个种群由 $n$ 个个体组成。本文遗传算法即对这 $n$ 个初始串结构进行迭代。

c)适应度函数计算。选取测试集数据均方误差平方的倒数作为适应度函数：

$$f(x)=\frac{1}{SE}=\frac{1}{sse(\hat{T}-T)}=\frac{1}{\sum_{i=1}^{n}(\hat{t}_i-t_i)^2}$$

其中:$\hat{T}=\{\hat{t}_1,\hat{t}_2,\ldots\hat{t}_n\}$ 为测试集的预测值；$T=\{t_1,t_2,\ldots t_n\}$ 为测试集的真实值；$n$ 为测试集样本数目。

d)选择操作。该步骤选用比例选择算子。

计算种群所有个体适应度之和为

$$F=\sum_{k=1}^{n_r} f(X_k),k=1,2,\ldots,n$$

计算种群个体相对适应度，作为个体被选中并遗传到下代种群的概率：

$$p_k=\frac{f(X_k)}{F},k=1,2,\ldots,n$$

采用模拟赌轮选择法，随机产生（0, 1）之间的数从而确定每个个体被选中的次数。适应度越大则该个体被选择的机会就越大。如果该个体能够被多次选择，那么它的遗传基因就会在种群中扩大，则该个体被选择到优化后的自变量个体概率就越大。

e)交叉操作。采用单点交叉算子实现自变量的压缩降维，算数交叉算子对 BP 神经网络权值和阈值进行优化。

f)变异操作。采用单点变异算子实现输入自变量的降维，非均匀变异算子对 BP 神经网络权值和阈值进行优化。

g)优化结果输出。经过多次迭代，得到最能代表输入输出关系的变量组合。

h)选择训练集与测试集。经过遗传算法对自变量降维后获得对应的训练集与测试集，用于 OCSVM 模型进行异常检测。

本文使用遗传算法对 OCSVM 参数 v 和核函数参数 g 进行寻优。研究发现 OCSVM 模型优劣的主要影响因素是参数 v 和核函数参数 g 的取值，应用遗传算法对 v 和 g 进行寻优，取得最优解，提高模型的检测准确率。

根据已有文献对 GA 计算复杂度的研究[14]，假定在 t 代时，坏模式生存下来的期望个数由二项式分布的均值给出。当遗传算法经过时间 $S_1$ 到达满足条件的解时，有

$$S_1=0.5(1-2h+\sqrt{(2h-1)^2-(8/\lambda)\ln(y_i/y_f)}\,)$$

其中: λ 和 h 是与遗传算法模式可靠性有关的常数[14]。

对于 OCSVM 来讲，求得满意解的时间复杂度 $S_2$ 最坏可以达到 $o(n^3)$，其中 n 是支持向量的个数。GA-OCSVM 方法的复杂度，与遗传算法中个体行为变化的概率相关[14]，而 SVM 的复杂度虽然没有固定的比例，但与支持向量的个数多少和训练集的大小有关，所以 OCSVM 算法复杂度容易受所选取训练集影响。

同时由于 GA 的引入，需要训练的 OCSVM 数量会有所增加，故相应的训练时间会有所延长，但是结构的优化和训练过程是离线进行的，不会影响 GA-OCSVM 的在线实时应用。以增加离线优化时间为代价换取 OCSVM 最优分类性能是值得的，所以本文使用遗传算法对 OCSVM 模型的参数进行优化。

## 4　基于 OCSVM 双轮廓异常检测模型

采用 OCSVM 分别构建功能控制行为的异常 OCSVM 模型和正常 OCSVM 模型，模拟系统通信的异常模式和正常模式，通过协同判别实时发现网络中的异常。双轮廓模型的实时协同判别流程如图 5 所示。

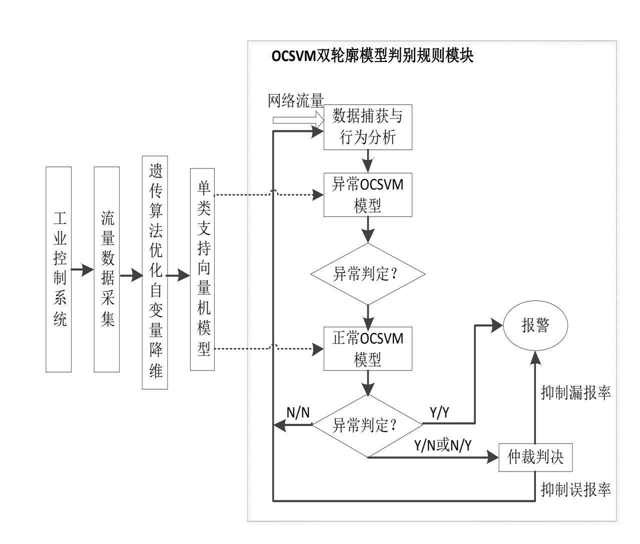



图 5　基于双轮廓模型的异常检测方法实时判别流程

实时协同判别引擎实时捕获并提取功能控制行为信息，以此作为模型的输入数据进行异常判定。双轮廓模型的协同判别机制简述如下：

a）若异常 OCSVM 模型判定为“正常”，同时正常 OCSVM 模型也判定为“正常”，则最终结果为“正常”；

b）若异常 OCSVM 模型判定为“异常”，同时正常 OCSVM 模型也判定“异常”，则最终结果为“异常”；

c）若异常 OCSVM 模型与正常 OCSVM 模型判定结果不一致，则需要进行进一步的仲裁判决，仲裁判决拟考虑误报率和漏报率两个因素，拟构建不同报警的影响权值，完成最终的异常判定。

## 5 实验验证与分析

为验证本文提出的基于 OCSVM 异常检测模型，搭建仿真平台，提取工控流量数据，使用 Wireshark 软件截获数据报文。

利用 MATLAB 神经网络工具箱及遗传算法工具箱提供的函数，对遗传算法优化自变量降维在 MATLAB 环境实现。提取 1000 条工业数据网络的 Modbus/TCP 数据，进行[0, 1]归一化处理后，采用其中的 700 条数据作为训练集，其余 300 条数据作为测试集进行遗传算法的优化操作。程序运行后，种群适应度函数进化曲线如图 6 所示。

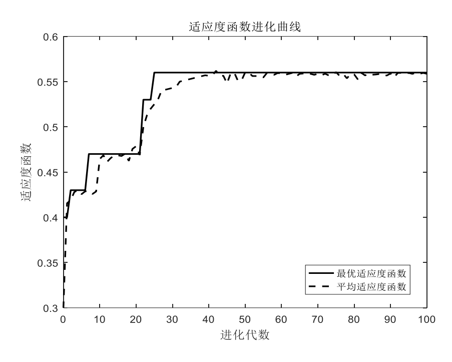



图 6 自变量降维种群适应度函数进化曲线

从上述结果看出，经降维后，筛选出一组自变量。优化后参与建模的输入自变量个数为全部输入自变量个数的一半。对比优化筛选前后的 BP 网络测试结果，发现，当选用 11 维输入自变量进行建模时，预测准确率得到改善和提升。同时，建模时间由 24.914s 减少为 4.641s，这表明使用遗传算法对输入自变量进行压缩降维后，建模时间缩短很多，证明采用该方法的有效性。

对 OCSVM 构建的双轮廓模型异常检测算法的验证采用所抓取 1000 条数据包中 600 条数据用于对所建模型的训练，其余 400 条数据用于测试。在不使用遗传算法优化处理时测试集的实际分类和预测分类如下图 7 所示，分类正确率为：$Accuracy = 93.75\%$。经过遗传算法优化后测试集的实际分类和预测分类如下图 8 所示，分类正确率为：$Accuracy = 98.00\%$。

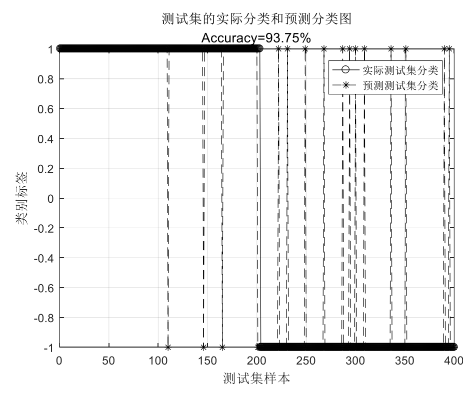



图 7 OCSVM 异常模型测试集检测结果

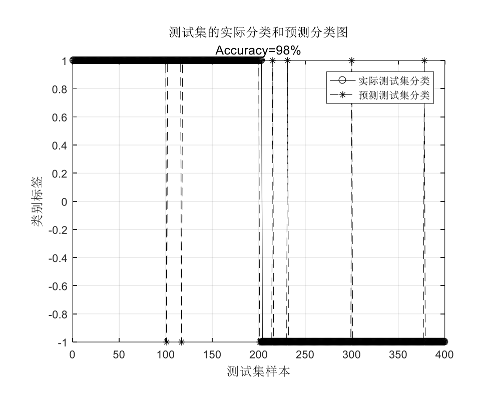



图 8 GA-OCSVM 双轮廓模型测试集检测结果

本文为验证所提异常检测方法的有效性，将遗传算法优化的 OCSVM 双轮廓模型与支持向量机算法、BP 算法、OCSVM 算法进行对比，采用相同的经过 Wireshark 软件截获 600 数据报文作为训练数据，另外 400 条数据作为测试集对各算法进行网络异常检测的验证，通过仿真实验与 GA-OCSVM 实验结果对比，结果如表 1 所示。

表 1 各算法性能对比

| 算法 | 测试集准确率 | 检测时间 |
|---|---|---|
| BP | 85.25% | 17.352s |
| SVM | 96.50% | 5.975s |
| OCSVM | 93.75% | 24.914s |
| GA-OCSVM | 98.00% | 4.641s |

可以看出几种算法对测试集的检测准确率都达不到 100%，但是 GA-OCSVM 的检测准确率能达到 98.00%，远远高于其他几种算法，表明本文提出的经遗传算法优化的 OCSVM 双轮廓模型通过实时协同判别机制能有效降低异常检测的漏报率和误报率，使得检测准确率得到提高。同时经遗传算法优化后输入自变量维度降低，使得 OCSVM 模型检测时间缩短，泛化能力更强，灵活性更高。GA-OCSVM 双轮廓异常检测模型能更好地解决工业控制网络中正常数据多、异常数据少、输入自变量维度高影响检测准确率的问题，更适用于实际工控网络。

## 6 结束语

本文针对工控网络 Modbus 工业总线协议及工控数据样本相对于传统 IP 网络的特殊性及数据分布不均衡性，利用 OCSVM 算法分别构建正常 OCSVM 模型和异常 OCSVM 模型，即双轮廓模态，模拟系统通讯的正常模式和异常模式，实现了工控系统的异常检测。同时本文将遗传算法优化自变量降维应用于工控网络，实现了对输入自变量的优化处理，抑制 OCSVM 模型出现过的拟合现象及分类准确率低的问题，提高了异常检测的精度，缩减了建模时间。通过仿真验证了本文提出算法对工控网络异常检测的有效性，在工控异常检测算法具有较大的应用价值。

## 参考文献：

[1] 崔君荣，尚文利，万明，等. 基于半监督分簇策略的工控入侵检测 [J]. 信息与控制, 2017, 46 (4): 462-468. (Cui Junrong, Shang Wenli, Wan Ming, *et al.* Intrusion detection of industrial control based on Semi-supervised clustering strategy [J]. Information and Control, 2017, 46 (4): 462-468. )

[2] Caselli M, Zambon E, Kargl F. Sequence-aware Intrusion Detection in Industrial Control Systems [C]// Proc of the 1st ACM Workshop on Cyber-Physical System Security. New York: ACM Press, 2015: 13-24.

[3] 尚文利，安攀峰，万明，等. 工业控制系统入侵检测技术的研究及 发展综述 [J]. 计算机应用研究, 2017, 34 (2): 328-333. (Shang Wenli, An Panfeng, Wan Ming, *et al.* Research and development overview of intrusion detection technology in industrial control system [J]. Application Research of Computers, 2017, 34 (2): 328-333. )

[4] 赵辉，房至一，李万龙，等. 基于失效检测算法的容忍入侵系统 [J]. 吉林大学学报：信息科学版, 2011, 29 (4): 349-356. (Zhao Hui, Fang Zhiyi, Li Wanlong, *et al.* Intrusion tolerance system based on failure detector algorithm [J]. Journal of Jilin University (Information Science Edition) , 2011, 29 (4): 349-356. )

[5] 陈善学，杨政，朱江，等. 一种基于累加 PSO-SVM 的网络安全态势预测模型 [J]. 计算机应用研究, 2015, 32 (6): 1778-1781. (Chen Shanxue, Yang Zheng, Zhu Jiang, *et al.* Network security situation prediction method based on PSO-SVM [J]. Application Research of Computers, 2015, 32 (6): 1778-1781. )

[6] Knowles W, Prince D, Hutchison D, *et al.* A survey of cyber security management in industrial control systems [J]. International Journal of Critical Infrastructure Protection, 2015, 9: 52-80.

[7] Maglaras L A, Jiang J, Cruz T. Integrated OCSVM mechanism for intrusion detection in SCADA systems [J]. Electronics Letters, 2014, 50 (25): 1935-1936.

[8] Maglaras L A, Jiang J. OCSVM model combined with K-means recursive clustering for intrusion detection in SCADA systems [C]// Proc of International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness. 2014: 133-134.

[9] Cai Lianfang, Tian Xuemin, Zhang Ni. Process fault detection method using time-structure KICA and OCSVM [J]. Journal of Tsinghua University, 2012, 52 (9): 1205-1209+1217. A. Almalawi,

[10] Erez N, Wool A. Control variable classification, modeling and anomaly detection in Modbus//TCP SCADA systems [J]. International Journal of Critical Infrastructure Protection, 2015, 10: 59-70.

[11] Wan Ming, Shang Wenli, Zeng Peng. Double Behavior Characteristics for One-class Classification Anomaly Detection in Networked Control Systems [J]. IEEE Trans on Information Forensics & Security, 2017, 3011 -3023.

[12] 李超，蔡宇晴，贾凡，等. 工业控制系统中基于单类支持向量机异常检测方法研究 [J]. 微型机与应用, 2017, 36 (23): 9-12. (Li Chao, Cai Yuqing, Jia Fan, *et al.* Research on anomaly detection based on one-class support vector machine in industrial control systems [J]. Smart Industry and Information Security, 2017, 36 (23): 9-12. )

[13] R. R. R. Barbosa, R. Sadre, A. Pras. Flow whitelisting in SCADA networks [J]. International Journal of Critical Infrastructure Protection, 2013, 6 (3): 150-158.

[14] 张宇山. 进化算法的收敛性与时间复杂度分析的若干研究 [D]. 广州：华南理工大学, 2013. (Zhang Yushan. Some studies on the convergence and time complexity analysis of evolutionary algorithms [D] , Guangzhou: South China University of Technology, 2013. )